UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/601,443	06/23/2003	Eduard Bergmann	KOA 0233 PUS (R 1420)	7995

22045 7590 01/25/2007

BROOKS KUSHMAN P.C.
1000 TOWN CENTER
TWENTY-SECOND FLOOR
SOUTHFIELD, MI 48075

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/601,443	Applicant(s) BERGMANN ET AL.	
	Examiner Samson B. Lemma	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 November 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on November 2, 2006. **All independent claims 1, 3, 5 and 8** are amended. Claims 1-9 **are pending/examined.**

Response to Arguments

2. Applicant's remark/arguments filed on November 2, 2006 regarding **claims 1-9** have been fully considered but they are not persuasive.

Applicant argument is based on the reference used in rejecting the corresponding limitation recited in the independent claims 1, 3, 5 and 8. Applicant in particular argued that the limitations which is now added in the independent claims are not disclosed by the reference used in the record namely, King.

In order to support his argument, Applicant wrote the following.

"In contrast, King describes data modules for a trainable transmitter in which the data modules are assigned to respective objects and respectively include data necessary to generate codes for the respective objects. The data for generating a code for an object may include a cryptographic algorithm. King describes a cryptographic algorithm is one used for generating a rolling code but is not used for generating a fixed code (see col. 2, lines 29-41 of King). In the case of a fixed code, the code is not "encrypted" (see col. 2, lines 38-41 of King). As such, a cryptographic algorithm described by King is an algorithm used to generate a code and is similar in function to the claimed symmetric encoding method which uses an encryption parameter to generate data. However, King does not teach or suggest an encryption algorithm as claimed which would be further used to encrypt a generated rolling code (which has been generated using a cryptographic algorithm as described by King) or a fixed code (which has been generated without the use of a cryptographic algorithm as described by King)."

Examiner disagrees with the above argument.

Examiner would point out that the on column 1, lines 43-45, King disclosed that the **cryptographic algorithm is also an encryption algorithm**. Furthermore, the claim language does not explicitly recites, what has been argued by the applicant. In particular the independent claims which is recited as having encryption algorithm different from the symmetric encoding method, does not explicitly recite that, this **particular encryption algorithm is used to further encrypt the code generated by the cryptographic algorithm of King, which applicant suggested is equivalent to the symmetric encoding method of the claim**.

Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In order to show how each and every limitation of the independent claim/s is disclosed by the reference after the claims are amended, the examiner would point out the following.

As per independent claims 1, 3, 5 and 8 **King discloses a keyless authorized access control system**, [Abstract, figure 1 & 2] **the system comprising**:

- **At least two object modules,**[Figure 2, ref. Num "44a" and "44b", "receiving systems" & column 3, lines 34-47] **each object module** [figure 2, ref. Num "44a" and "44b"] **being assigned to a respective object** ["garage door opener object & home security system object] (On column 3, lines 34-47 and the corresponding figure 2, the following has been recited. "Upon receiving the digital code, the receiving system 44a, which met to be one object module, activates the system, such as opening or closing the garage door which met to be the respective object for object module 44a. When the user activates the second switch 34b, the code-generation circuitry 30 accesses the second data module 14b, which met to be the other object modules and generates a second digital code, based upon a second cryptographic algorithm. This second digital code is transmitted via the antenna 38 by the oscillator 36, possibly at a second frequency and utilizing a second modulation scheme. This wireless signal is received by the second receiving system 44b/the other object module, such as a home security system which met to be the respective object for object module 44b which activates the system based upon receiving the proper digital code.") **and**

- **At least one identification device**,[Figure 1, ref. Num "10/transmitter system" or figure 1, ref. Num "12", "trainable transmitter"] (Transmitter system shown on figure 1, ref. Num 10 met the identification device) **each identification device having a microprocessor** [column 1, lines 48-60] **and a memory element** [column 2, lines 21-28];

- **wherein each identification device and the object modules have respective bidirectional data communications links between them** [column 3, lines 28-47, figure 1 and 2, see, in particular "transmission via antenna" on column 3, line 42] **for communicating encoded data, the data communicated between an identification device and each object module being encoded by an encryption algorithm and a symmetric encryption method which uses an encryption parameter, wherein encryption algorithms and encryption parameters are uniquely assigned to the object modules** [column 3, lines 28-36 , column 3, lines 12-17, column 1, lines 48-60] (On column 3, lines 28-36, the following has been disclosed, In operation, referring to FIGS. 1 and 2, when the user activates one of the switches 34a, for example, the code-generation circuitry 30 accesses the corresponding data module 14a to obtain the code-generation algorithms and other data. The code-generation circuitry 30 then generates the appropriate digital code, which is transmitted via the antenna 38 by the oscillator 36. This wireless signal is received by the receiving system 44a, such as a garage door opener. And this meets the limitation "communicating encoded data, the data communicated between an identification device and an object module being encoded using an encryption algorithm that performs encryption method which uses an encryption parameter respectively assigned to the object module". Furthermore on column 3, lines 12-17, the following has also been recited, "In operation, a user initially selects one of the data modules 14a-e which corresponds to the garage door opener (or other security system) that the user wishes the vehicle transmitter system 10 to operate. The selected data module 14 must have the same cryptographic algorithm, frequency, modulation, etc. that the receiving garage door opener receiver utilizes." And this meets the limitation of "encryption algorithm that performs a symmetric encryption method"]

- **wherein the memory element of each identification device stores at least two different encryption algorithms and at least two different encryption parameters including the encryption algorithms and the encryption parameters assigned to the object modules** [column 1, lines 16-22 and column 2, lines 21-37] (On column 1, lines 16-22 the following has been recited. "The current trainable transmitters pre-store a plurality of cryptographic algorithms allowing the trainable transmitter to be universal" and this meets the limitation of each identification device stores at least two different encryption algorithms. This provides convenience to the consumer by allowing the trainable transmitter to be compatible with many home products, such as garage door openers. Furthermore, the following has been recited on column 2, lines 30-37.

"The data modules 14a-e /which is part and parcel the trainable transmitters each contains different data necessary to generate a digital code for a different security system. For example, each data module 14a-e contains a cryptographic algorithm for generating a rolling code and an indication of the frequency at which the wireless signal containing the digital code is to be generated. The data module 14 may also include other information regarding the modulation protocol of the wireless signal to be sent" and this meets the limitation each identification device stores at least two different encryption algorithms and at least two different encryption parameters including the encryption algorithms and the encryption parameters assigned to the object modules.)

wherein the microprocessor of an identification device selects one of/from the stored encryption algorithms and encryption parameters the encryption algorithm and the encryption parameter assigned to an object module to be used with the symmetric encryption method for encoding the data to be communicated between the identification device and an object module.[Column 1, lines 48-60 and column 2, lines 50-61] (The present invention provides a re-configurable trainable transmitter including a removable plug-in data module which contains a cryptographic algorithm and the other information necessary for generating a wireless signal containing a code associated with a specific security system. The trainable transmitter generally comprises a transmitter and code-generation circuitry, such as a microprocessor. The microprocessor generates a digital code based upon the data in the data module, including the cryptographic algorithm. The microprocessor determines a digital code based upon the cryptographic algorithm and the transmitter generates a wireless signal including the digital code at a frequency also specified by the data module and this meets the recitation of the above limitation.)

As it has been recited above each and every limitation of the claims has been disclosed by the reference on the record. The rejection is maintained until the applicant further amends and successfully overcomes the ground of rejection set forth in this office action. Finally, **examiner would suggest the applicant to show how the encryption algorithm is different from the symmetric encryption method in the claim itself.** This is because before the claim was amended the limitation indicated that the encryption algorithm is that performs a symmetric encryption method, however it is now amended as if these two terms are different.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4 **Claims 1-9** are rejected under 35 U.S.C. 102(e) as being anticipated by **Joseph David King** (hereinafter referred as **King**)(U.S. Patent No. 6,556,681 B2) (filed on August 26, 1998)

5. **As per independent claims 1, 3, 5 and 8** **King discloses a keyless authorized access control system**, [Abstract, figure 1 & 2] **the system comprising**:

- **At least two object modules,**[Figure 2, ref. Num "44a" and "44b", "receiving systems" & column 3, lines 34-47] **each object module** [figure 2, ref.

Num “44a” and “44b”] **being assigned to a respective object** [“garage door opener object & home security system object] (On column 3, lines 34-47 and the corresponding figure 2, the following has been recited. “Upon receiving the digital code, the receiving system 44a, which met to be one object module, activates the system, such as opening or closing the garage door which met to be the respective object for object module 44a. When the user activates the second switch 34b, the code-generation circuitry 30 accesses the second data module 14b, which met to be the other object modules and generates a second digital code, based upon a second cryptographic algorithm. This second digital code is transmitted via the antenna 38 by the oscillator 36, possibly at a second frequency and utilizing a second modulation scheme. This wireless signal is received by the second receiving system 44b/the other object module, such as a home security system which met to be the respective object for object module 44b which activates the system based upon receiving the proper digital code.”) and

- **At least one identification device**,[Figure 1, ref. Num “10/transmitter system” or figure 1, ref. Num “12”, “trainable transmitter”] (Transmitter system shown on figure 1, ref. Num 10 met the identification device) **each identification device having a microprocessor** [column 1, lines 48-60] **and a memory element** [column 2, lines 21-28];

- **wherein each identification device and the object modules have respective bidirectional data communications links between them** [column 3, lines 28-47, figure 1 and 2, see, in particular “transmission via antenna” on column 3, line 42] **for communicating encoded data, the data communicated between an identification device and each object module being encoded by an encryption algorithm and a symmetric encryption method which uses**

an encryption parameter, wherein encryption algorithms and encryption parameters are uniquely assigned to the object modules [column 3, lines 28-36 , column 3, lines 12-17, column 1, lines 48-60] (On column 3, lines 28-36, the following has been disclosed, In operation, referring to FIGS. 1 and 2, when the user activates one of the switches 34a, for example, the code-generation circuitry 30 accesses the corresponding data module 14a to obtain the code-generation algorithms and other data. The code-generation circuitry 30 then generates the appropriate digital code, which is transmitted via the antenna 38 by the oscillator 36. This wireless signal is received by the receiving system 44a, such as a garage door opener. And this meets the limitation "communicating encoded data, the data communicated between an identification device and an object module being encoded using an encryption algorithm that performs encryption method which uses an encryption parameter respectively assigned to the object module". Furthermore on column 3, lines 12-17, the following has also been recited, "In operation, a user initially selects one of the data modules 14a-e which corresponds to the garage door opener (or other security system) that the user wishes the vehicle transmitter system 10 to operate. The selected data module 14 must have the same cryptographic algorithm, frequency, modulation, etc. that the receiving garage door opener receiver utilizes." And this meets the limitation of "encryption algorithm that performs a symmetric encryption method"]

- **wherein the memory element of each identification device stores at least two different encryption algorithms and at least two different encryption parameters including the encryption algorithms and the encryption parameters assigned to the object modules** [column 1, lines 16-22 and column 2, lines 21-37] (On column 1, lines 16-22 the following has been recited. "The current trainable transmitters pre-store a plurality of cryptographic algorithms allowing the trainable transmitter to be universal" and this meets the limitation of each identification device stores at least two different encryption algorithms. This provides convenience to the consumer by allowing the trainable transmitter to be compatible with many home products, such as garage door openers. Furthermore, the following has been recited on column 2, lines 30-37. "The data modules 14a-e /which is part and parcel the trainable transmitters each contains different data necessary to generate a digital code for a different security system. For example, each data module 14a-e contains a cryptographic algorithm for generating a rolling code and an indication of the frequency at which the wireless signal containing the digital code is to be generated. The data module 14 may also include other information regarding the modulation protocol of the wireless signal to be sent" and this meets the limitation each identification device stores at least two different encryption algorithms and at least two different encryption parameters including the encryption algorithms and the encryption parameters assigned to the object modules.)

wherein the microprocessor of an identification device selects one of/from the stored encryption algorithms and encryption parameters the encryption algorithm and the encryption parameter assigned to an object module to be used with the symmetric encryption method for encoding the data to be communicated between the identification device and an object module.[Column 1, lines 48-60 and column 2, lines 50-61] (The present invention provides a re-configurable trainable transmitter including a removable plug-in data module which contains a cryptographic algorithm and the other information necessary for generating a wireless signal containing a code associated with a specific security system. The trainable transmitter generally comprises a transmitter and code-generation circuitry, such as a microprocessor. The microprocessor generates a digital code based upon the data in the data module, including the cryptographic algorithm. The microprocessor determines a digital code based upon the cryptographic algorithm and the transmitter generates a wireless signal including the digital code at a frequency also specified by the data module and this meets the recitation of the above limitation.)

6. **<u>As per dependent claims 2 & 4</u> King** discloses a system as applied to claims above. **Furthermore King** discloses the system wherein: the encryption algorithm to be used for encoding the data to be communicated between the identification device and an object module is assigned by the identification device to the object module during a single initialization process between the identification device and the object module. [Column 1, lines 48-60 and column 3, lines 28-47]

7. **<u>As per dependent claims 6 & 9</u> King** discloses a system as applied to claims above. **Furthermore King** discloses the system wherein: the encryption algorithms stored in the memory element are configurable and replaceable through a programming interface. [column 1, lines 48-60, figure 1 & 2 and column 2, lines 29-61]

8. **<u>As per dependent claim 7</u> King** discloses a system as applied to claims above. **Furthermore King** discloses the system wherein: the memory element is integrated in the microprocessor. [Column 1, lines 48-60 , figure 1 & 2 and column 2, lines 45-61]

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
01/10/2007

Gilberto
GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100